Merancang Software Virus Komputer Penghancur File Gambar

Rina Candra Noor Santi
Fakultas Teknologi Informasi, Universitas Stikubank Semarang
email : rina@unisbank.ac.id

Abstrak : Pesatnya perkembangan teknologi komputer dan internet pada saat ini juga telah memacu perkembangan kejahatan di dunia maya tersebut terutama virus komputer yang telah menyebabkan kerugian bagi banyak pihak.sehingga kita mencoba untuk berpartisipasi dalam menganalisa dan merancang pembuatan virus komputer menggunakan bahasa pemrograman vbscript. Dimana virus tersebut menyerang file gambar (image) dan dokumen. Tujuan dari pembuatan virus komputer ini agar bisa menjadi salah satu wacana bagi para pengguna komputer atau internet untuk mewaspadai akan bahaya virus komputer yang bisa datang melalui disket, flashdisk maupun internet. Sekaligus bisa mengantisipasi kerusakan yang diakibatkan oleh virus komputer.

Kata kunci : virus komputer, internet, vbscript

PENDAHULUAN

Saat ini, kita sebagai salah satu konsumen atau pengguna jasa komputer dan jaringan tidaklah asing dan bahkan sering mendengar istilah "virus". Dimana hal tersebut terkadang membuat kita sebagai pengguna komputer menjadi jengkel, resah atau bahkan timbul kekhawatiran data-data yang kita miliki akan rusak atau hilang jika sewaktu-waktu terinfeksi virus. Belum lagi jika virus tersebut menyerang sistem komputer kita yang bisa mengakibatkan komputer menjadi crash dan harus diinstal ulang.

Virus komputer bisa diartikan sebagai suatu program komputer biasa, tetapi memiliki perbedaan yang mendasar dengan program-program lainnya. Virus dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya.

Piranti/Perangkat Lunak

Menurut *Roger S. Pressman, Ph.D. ,2002, Rekayasa Perangkat Lunak,* Perangkat Lunak merupakan (1) sebuah perintah (program komputer) yang bila dieksekusi memberikan fungsi dan unjuk kerja seperti yang diinginkan. (2) Struktur data yang memungkinkan program memanipulasi informasi secara proporsional, dan (3) Dokumen yang menggambarkan operasi dan kegunaan program.

Karakteristik Perangkat Lunak

Menurut *Roger S. Pressman, Ph.D. ,2002, Rekayasa Perangkat Lunak,* Perangkat lunak lebih merupakan elemen logika dan bukan merupakan elemen sistem fisik. Dengan demikian, perangkat lunak memiliki ciri yang berbeda dari perangkat keras.

1. Perangkat lunak dibangun dan dikembangkan, tidak dibuat dalam bentuk yang klasik.
2. Perangkat lunak tidak pernah usang/rentan terhadap pengaruh lingkungan yang merusak yang menyebabkan perangkat keras menjadi usang.
3. Sebagian besar perangkat lunak dibuat secara custom-built, serta tidak dapat dirakit dari komponen yang sudah ada.

Virus Komputer

Pengertian Virus *(www.indovirus8.com)*

Virus Komputer adalah sebuah program komputer biasa yang mempunyai rutin atau prosedur untuk mengcopykan sebagian atau seluruh bagian programnya ke dalam program lain, sehingga program yang ditularinya berjalan tidak sebagaimana mestinya, misalnya program berjalan lebih lambat dari biasanya atau malah tidak berjalan sama sekali. Istilah "Virus" dikarenakan adanya kemiripan antara penyebaran program virus kedalam program-

program lain dan mekanisme penyebaran virus biologis kedalam sel-sel makhluk hidup, sehingga dengan persamaan ini dapat ditarik kesimpulan dan dibuatkan suatu tabel persamaan antara Virus Komputer dengan virus biologis, sehingga dapat kita lihat persamaan antara keduanya.

Berikut ini akan ditunjukan suatu tabel persamaan antara Virus Biologis Dengan Virus Komputer :

Tabel 1. Persamaan Virus Komputer dengan Virus Biologis

Virus Biologis	Virus Komputer
Merusak sel-sel tertentu dari mahluk hidup	Merusak file-file tertentu dari komputer (misalkan : semua file.COM atau file.EXE)
Mengubah sifat-sifat bawaan dari sel	Mengubah cara kerja program asli (Eg. Program jadi lambat)
Sebuah sel yang sakit hanya sekali diserang oleh virus yang sama	Kebanyakan Virus Komputer menularkan program hanya sekali
Didalam sel-sel yang telah diserang virus, tumbuh virus-vrus baru	Program yang sudah tertular virus dapat menularkan ke program-program lainnya
Sebuah organisme yang sakit tidak segera menunjukan gejala sakit	Sebuah program yang tertular dapat berfungsi normal untuk waktu yang lama
Tidak semua sel yang berhubungan dengan virus, ditulari	Program-program dapat dibuat kebal terhadap virus-virus tertentu
Virus-virus menunjukan mutasi menghasilkan ciri-ciri baru	Program-program virus dapat berubah (Mutasi) dengan sendirinya, sehingga gagal mendeteksinya

Kriteria Virus

Menurut IR.Hartojo Salim, dari bukunya "*Virus Komputer, teknik pembuatan dan langkah-langkah pembuatannya*", Suatu program yang disebut virus baru dapat dikatakan adalah benar benar virus apabila minimal memiliki 5 kriteria :

1. Kemampuan suatu virus untuk mendapatkan informasi
2. Kemampuannya untuk memeriksa suatu program
3. Kemampuannya untuk menggandakan diri dan menularkan

   Beberapa cara umum yang dilakukan oleh virus untuk menulari atau menggandakan dirinya adalah:

   a. Mengubah atau menghapus nama file yang ditulari kemudian diciptakan suatu file menggunakan nama itu dengan menggunakan virus tersebut.

   b. Program virus yang sudah dieksekusi atau diload ke memori akan langsung menulari file-file lain dengan cara menumpangi seluruh file atau program yang ada.
4. Kemampuannya melakukan manipulasi
5. Kemampuannya untuk menyembunyikan diri.

Klasifikasi Virus Komputer
(www.indovirus8.com)

a. Klasifikasi Virus Komputer Secara Umum

1. Virus Boot Sector

Virus Boot Sector merupakan virus yang memanfaatkan gerbang hubungan antara komputer dan media penyimpanan, sebagai tempat penyebarannya.

2. Virus File

Dalam penyebarannya virus ini memanfaatkan file-file eksekusi yang dapat diproses langsung dalam dos command line, seperti file-file COM, File EXE, File BAT, dan File SYS.

Pada teknologi baru pembuatan virus komputer, virus ini juga dapat

menyerang file Dokumen dalam Windows dengan extensi DOC, yang biasa disebut Virus Macro. Virus Komputer ini biasa dirtulis dengan Visual Basic, Java Script, VBScript, Visual C++ dan lain sebagainya sehingga dapat disebarkan melalui Internet dalam bentuk E-mail Attachment

3. Virus Hybrid

Virus Komputer jenis ini disebut juga Virus Komputer automodifikasi yang mempunyai kemampuan untuk menyerang atau menginfeksi Boot record juga dapat menginfeksi file-file dalam disket. Virus-virus ini biasanya mempunyai kemampuan untuk bersembunyi yang lebih baik dari pada virus boot record atau pun virus file.

b. Klasifikasi Menurut Cara Penularan Atau Penyebaran

Menurut cara penularan atau penyebarannya virus dibagi menjadi 3 bagian umum yaitu :

1. Appending (Menempel)
2. Overwriting (Menimpa)
3. Spawning / Companion

c. Klasifikasi Menurut Rutin Aktivasi

1. Virus Jinak

Virus dengan rutin atau tugas yang dibebankan kepadannya tidak melakukan aksi-aksi destruktif.

2. Virus Ganas

Yang termasuk rutin atau aksi yang merugikan atau berbahaya dari virus ini seperti menghapus file, memformat harddisk dan membebani server atau attachment Email.

3. Virus Destruktif

Virus Komputer jenis destruktif ini daya rusaknya sangat besar dan juga dapat menghancurkan sofware maupun hardware.

Siklus Hidup Virus

Menurut IR.Hartojo Salim, dari bukunya "*Virus Komputer, teknik pembuatan dan langkah-langkah pembuatannya*", siklus hidup virus ada 4 macam yaitu :

1. Dormant phase (Fase Istirahat/Tidur)

   Pada fase ini virus tidaklah aktif. Virus akan diaktifkan oleh suatu kondisi tertentu, misalnya tanggal yang ditentukan, kehadiran program lain atau dieksekusinya program lain, dan sebagainya. Tidak semua virus melalui fase ini.

2. Propagation phase (Fase Penyebaran)

   Pada fase ini virus akan mengkopikan dirinya kepada suatu program atau ke suatu tempat dari media storage (baik harddisk, ram dan sebagainya). Setiap program yang terinfeksi akan menjadi hasil "klonning" virus tersebut (tergantung cara virus tersebut menginfeksinya).

3. Trigerring phase (Fase Aktif)

   Di fase ini virus tersebut akan aktif dan hal ini juga dipicu oleh beberapa kondisi seperti pada Dormant phase.

4. Execution phase (Fase Eksekusi)

   Pada Fase inilah virus yang telah aktif tadi akan melakukan fungsinya. Seperti menghapus file, menampilkan pesan-pesan, dan sebagainya.

Metode Analisis Program Virus *(www.vaksin.com)*

Biasanya ada Beberapa langkah yang dilakukan oleh para programmer dalam menganalisis atau membedah isi sebuah virus, hal ini dilakukan agar programmer bisa mengetahui metode, cara kerja termasuk pola penyerangan dari suatu virus komputer, agar bisa diketahui cara menangkal atau bisa dibuat program antivirusnya

Caranya adalah dengan metode Black Box Analysis, Dissasembly (dekompilasi) dan melihat jalannya virus dengan debugger. Tetapi dikarenakan keterbatasan ilmu pada penulis dan hanya programmer tingkat tinggi yang mengetahui atau mendalami seluk beluk tentang virus komputer. Maka penulis hanya menggunakan metode "***black box analysis***".

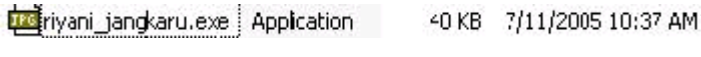
Pengujian Black-Box berfokus untuk mendapatkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsional untuk suatu program. Pengujian ini berusaha untuk menemukan kesalahan dalam kategori berikut: (1)fungsi-fungsi yang tidak benar atau hilang, (2)kesalahan interface, (3)kesalahan dalam struktur data atau akses database eksternal, (4)kesalahan kinerja, (5)inisialisasi dan kesalahan terminasi.

Cara yang mudah dalam hal ini adalah dengan melihat perubahan komputer secara langsung. Beberapa program tersedia untuk melihat perbedaan *state* komputer sebelum dan sesudah program sesuatu dijalankan (termasuk juga sebelum dan sesudah virus dijalankan). Program semacam ini bisa menunjukkan (1)file-file apa saja yang dibuat virus, dan (2)perubahan registry apa yang dilakukan oleh virus.

Sekilas tentang virus JPEG *(www.vaksin.com)*

Sejarah membuktikan bahwa virus yang berhasil tidak harus rumit atau berbelit-belit dalam bahasa pemrograman. Asalkan menggunakan rekayasa sosial yang tepat saja hasilnya tidak kalah atau bahkan lebih bagus daripada eksploitasi celah keamanan dengan programming yang rumit. Contoh virus JPEG yang pernah sukses pada masanya yaitu virus AnnaKournikova. Virus ini dibuat menggunakan tools Kalamar (VBSWG) untuk pembuat virus amatiran tetapi karena rekayasa sosialnya yang tepat (pada saat itu) dimana setiap orang akan tertarik untuk melihat gambar petenis cantik Rusia, Anna Kournikova maka penyebarannya sangat sukses dan mengalahkan virus lain yang programmingnya jauh pebih canggih dan rumit.

Virus Lokal yang tidak kalah suksesnya adalah virus Riani_Jangkaru [W32/Tabaru] atau Siti Nurhaliza [W32/Runitis] dan Asti Asnanta [W32/Astanta.A], virus ini dibuat dengan memanfaatkan "public figure" (orang yang berpengaruh atau terkenal) untuk menarik perhatian sehingga mereka yang awam terhadap virus komputer akan mudah terjebak menjalankan file bervirus yang mereka suguhkan.



Gambar 1. Contoh Tampilan Virus Riyani Jangkaru

Program yang Digunakan

Dalam perancangan sebuah virus komputer,diperlukan beberapa program antara lain :

1. ExeScript (Writing)

ExeScript merupakan sebuah program untuk menulis sebuah script atau bahasa pemrograman layaknya seperti notepad (program script editor bawaan windows). Program ini mendukung untuk penulisan sebuah file batch (.bat), bahasa javascript (.js) dan tentunya vbSript (.vbs) yang akan digunakan penulis untuk membuat program virus komputer. Selain itu program ini bisa meng-compile bahasa pemrograman yang telah penulis buat, menjadi sebuah bentuk file exe (file aplikasi yang siap untuk dijalankan).

2. IconChanger v 3.6

Program ini berfungsi untuk mengubah tampilan icon standart EXE menjadi icon yang kita inginkan dalam hal ini icon gambar (image). peran program ini sangat penting karena yang menentukan berhasil atau tidaknya program virus ini dalam hal social engineering (rekayasa sosial).

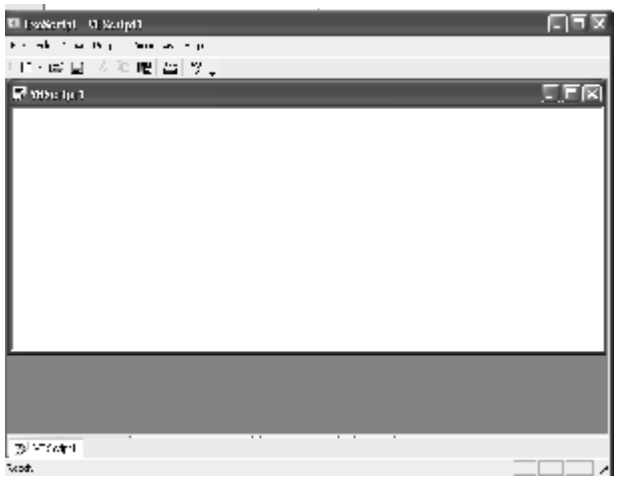
3. UPX (Packing)

UPX merupakan software untuk packing yang portable, flexible dan high-performance untuk digunakan. UPX juga dapat melakukan packing dalam beberapa format extensi file, seperti exe, scr, pif, dll dan lain-lain. Program ini melakukan kompresi rasio yang sangat bagus dan menawarkan decompression yang begitu cepat. File yang dipacking tidak memerlukan memory yang begitu banyak atau dukungan dari file-file lain. Selain memperkecil ukuran program UPX juga untuk menyembunyikan kode virus yang telah kita buat.

Penjelasan Program Yang Dipakai

a. Program EXEScript

Berikut adalah tampilan awal dari program ini ketika dijalankan.



Gambar 2 Tampilan Program XEScript

Untuk memulainya kita double klik icon ExeScript pada Desktop atau Start Menu. Selanjutnya Kita pilih **File → New → Vbscript** sampai keluar tampilan seperti gambar di atas di sini kita bisa langsung memulai untuk menuliskan script vbscript.

Untuk menyimpan script yang telah kita buat, bisa kita tekan tombol cepat **ctrl+s** atau kalau ingin langsung meng-compile project ke dalam bentuk .exe, kita tekan tombol **F9**.

b. IconChanger 3.6

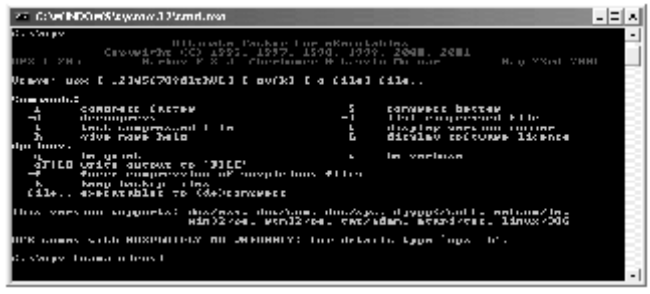
Untuk mengubah tampilan icon, kita bisa langsung klik kanan dari file virus yang telah kita buat dari windows explorer kemudian pilih change icon sampai keluar tampilan program seperti pada gambar di bawah ini :

Gambar 3. Tampilan Program IconChanger

Untuk mencari daftar icon-icon dari komputer, tekan tombol **search**. Selanjutnya, kita pilih salah satu gambar icon yang kita sukai dan tekan tombol **set**.

c. UPX

Jalankan file UPX dari Command Prompt. Caranya adalah ketik **cmd** dari **Start Menu → Run.** lalu pindahkan ke direktori tempat file upx itu berada dan ketik upx sampai keluar tampilan sebagai berikut:



Gambar 4. Tampilan Program UPX

Kemudian ketik upx spasi [nama virus] yang akan dipacking. Jika benar maka akan sampai keluar perbandingan kompresi sebelum dan sesudahnya.

Tampilan dan Efek Program Virus Setelah dijalankan

1. Penanda virus

   Virus ini memiliki tampilan awal seperti pada gambar di bawah ini :

Gambar 5. Tampilan Program Virus

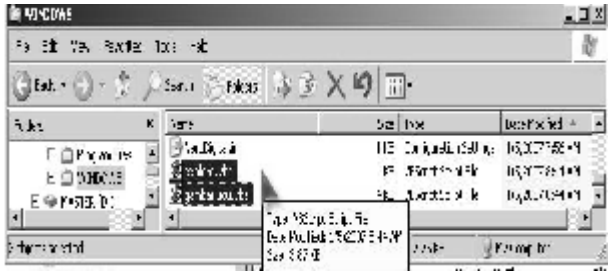
Virus ini penulis beri nama luculucu.exe**,** mempunyai ukuran file sebesar 10 kb. Untuk tampilan iconnya, menggunakan tampilan gambar JPEG.

2. Penggandaan Virus

   Setelah program virus ini dijalankan, dia akan membuat backup file di direktori windows, dansystem32, yang akan

dijalankan setiap kali windows dinyalakan. dengan memanipulasi register windows

Pada directory windows, virus membuat backup virus dengan nama explore.vbs dan gambarlucu.vbs, seperti pada gambar :

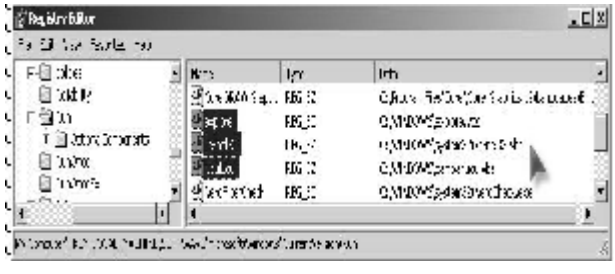


Gambar 6. BackUp Virus directory Windows

Sedangkan pada directory system32, virus membuat backup virus dengan nama kernel32.vbs, seperti pada gambar :

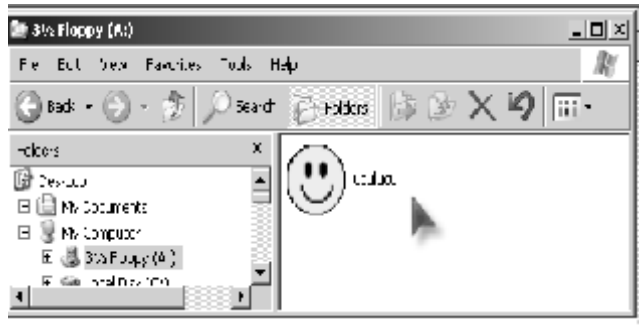
Gambar 7. BackUp Virus directory System32

Kemudian Virus akan membuat string di regedit yang akan menjalankan backup virus tersebut setiap saat, lihat pada gambar :



Gambar 8. String virus yang menunjukkan lokasi virus pada system di Regedit

Virus juga akan mengkopikan dirinya sendiri ke setiap drive yang ada termasuk disket dan flashdisk untuk menyebarkan dirinya. Berikut adalah gambar dari isi folder di drive A yang telah terdapat backup dari virus tersebut.



Gambar 9. BackUp Virus Di drive A

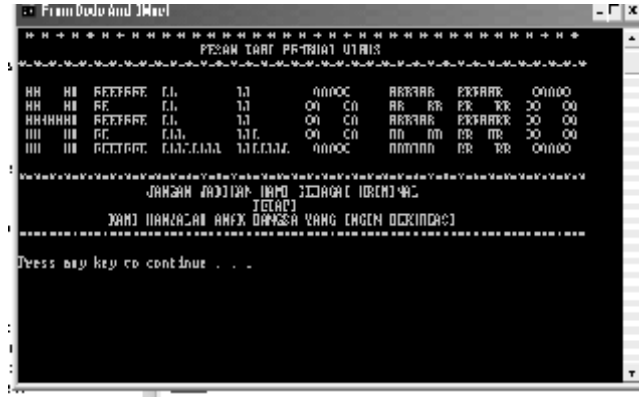
3. Manipulasi Virus

Rutin Manipulasi akan dijalankan atau ditampilkan oleh virus pada saat kondisi waktu terpenuhi yaitu sebagai berikut :

a. Menampilkan tulisan atau pesan

Gambar 10. Menampilkan Pesan

b. Menampilkan pesan ketika windows pertama kali booting



Gambar 11. Menampilkan Pesan Ketika Booting

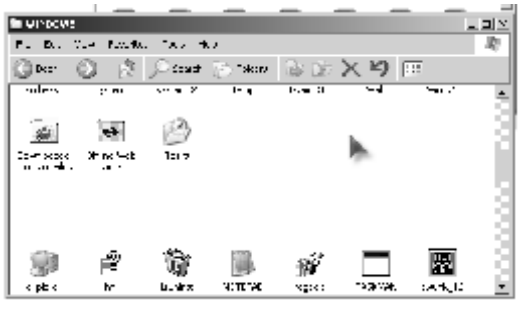
c. Merubah nama pemilik Windows (Registered Organization dan Owner) standard menjadi :

Gambar 12. Tampilan About Windows

d. Mencari dan menghapus file gambar (.jpeg, .bmp dan .gif)

Jika virus menemukan file gambar(image) ketika kita membuka explorer, maka otomatis file tersebut akan dihapus oleh virus. Berikut adalah gambar yang menunjukkan aktifitas virus yang berjalan ketika dia menemukan beberapa file gambar yang digunakan untuk wallpaper di direktori windows. Ketika kita masuk ke direktori tersebut., maka file gambar tersebut akan otomatis terhapus.

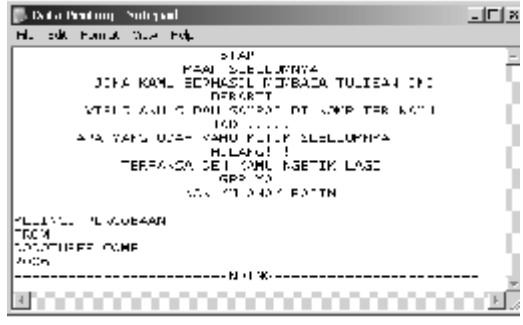
Gambar 13. Sebelum File gambar Dihapus



Gambar 14. Setelah File gambar Dihapus

e. Mencari dan memodifikasi(overwrite) file dokumen (.txt dan .doc)

virus tersebut menemukan sebuah file text (.txt dan .doc) ia akan meng-overwrite isi dari dokumen tersebut. Sehingga isi dokumen yang semula, akan berubah menjadi pesan dari virus, seperti pada gambar :



Gambar 15. file dokumen yang telah dimodifikasi virus

4. Pertahanan virus

Untuk mempersulit pembersihan virus komputer maka virus akan menonaktifkan beberapa fungsi windows seperti :

a. Mendisable atau menonaktifkan program regedit.

Hal ini dilakukan untuk mempersulit pembersihan program virus. Sehingga ketika user ingin membuka program registry editor (regedit) maka akan muncul tampilan pesan error sebagai berikut :

Gambar 16. Disabled registry editor

b. Mendisable atau menonaktifkan Task Manager (Ctrl+Alt+Del)

Berikut adalah tampilan ketika user mencoba mengakses tombol tersebut.

Gambar 17. Disabled Task Manager

c. Menonaktifkan fungsi Run Klik Kanan–Properties

Berikut adalah tampilan ketika user mencoba mengakses tombol tersebut.

Gambar 18. Disabled Run

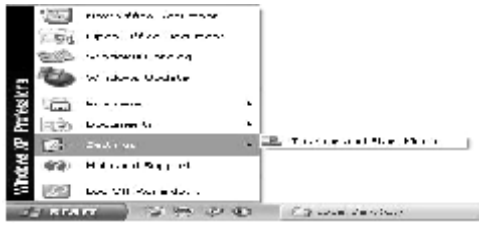
d. Menyembunyikan menu Folder Option

Berikut adalah tampilan ketika user mencoba mengakses tombol tersebut.

Gambar 19. Hidden Folder Option

e. Menyembunyikan Menu Control Panel – Search – Run - Shutdown

Berikut adalah tampilan ketika user mencoba mengakses tombol tersebut.



Gambar 20. Hidden Fungsi Windows

PENUTUP

Pembuatan virus komputer ini janganlah dianggap sebagai suatu kejahatan, tetapi agar kita bisa belajar untuk lebih waspada terhadap perkembangan dan penyebaran virus – virus komputer di dunia maya yang semakin hari semakin canggih dan sangat mengkhawatirkan, apalagi pembuatannya dengan menggunakan teknik "social Engineering" yang bisa menipu para pengguna awam. Pentingnya mengetahui dan mempelajari tentang sekuritas (keamanan) sistem komputer kita yang sudah ada saat ini agar tidak mudah terkena virus komputer serta bisa mengatasi permasalahan yang timbul berkaitan dengan virus komputer.

DAFTAR PUSTAKA

1. http://www.indovirus8.com
2. http://www.virologi.info
3. http://www.vaksin.com
4. Salim, IR.Hartojo. 1989. Virus Komputer, teknik pembuatan & langkah-langkah penanggulangannya. Andi OFFSET : Yogyakarta
5. Fajar Djunaedi EP, Bayu Prasetio. 2003. Trik Mendongkrak Performa Windows. PT. Elex Media Computindo : Jakarta
6. Synomadeus, DenyZip. 1997. Rahasia Teknik Pembuatan Virus Komputer. Andi OFFSET : Yogyakarta
7. Shadewa, Aat. 2006. Seni Pemrograman Virus menggunakan Visual Basic 6.0. DSI Publishing : Yogyakarta